

2000

# Is the Answer to Internet Addiction Internet Interdiction?

William H. Friedman

*University of Central Arkansas, [friedmanw@acm.org](mailto:friedmanw@acm.org)*

Follow this and additional works at: <http://aisel.aisnet.org/amcis2000>

---

## Recommended Citation

Friedman, William H., "Is the Answer to Internet Addiction Internet Interdiction?" (2000). *AMCIS 2000 Proceedings*. 226.  
<http://aisel.aisnet.org/amcis2000/226>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2000 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# Is the Answer to Internet Addiction Internet Interdiction?

William H. Friedman, Dept. of Marketing, Management, and Information Systems,  
University of Central Arkansas, Conway, AR, friedmanw@acm.org

## Abstract

The purposes of this paper are (1) to highlight problems concerning employee misuse of the Internet while on the job, (2) to provide an ethical and economic analysis of this phenomenon, but, more importantly, (3) to evaluate existing solutions and suggest new ones, and (4) to do justice to the points of view of employees engaged in this activity. When Internet usage is unrelated to the business or the defined position of an employee and is done on company time, there is at the very least a presumed decrease in productivity. That presumption will be evaluated below.

By reason of the employee's extraneous preoccupation with the Internet there is probably also a decrease in the amount of conscious attention given to the processing of company business problems, which the employee is paid to solve. There are also moral issues concerning the misuse of time, evasion of responsibility, and breach of employee-employer contract. Moreover the employer can incur additional expenses when company resources are not being used as intended. This can be construed as indirect theft on the part of the abusers.

## Terminology for Preciseness

To eliminate possible misunderstanding that might arise from different interpretations of potentially controversial terms, it would be useful to stipulate the following way in which such terms will be used:

1. Stealing is defined as "To take (the property of another) without right or permission" (American Heritage Electronic Dictionary, 1992).

2. Cyberslacking involves visiting pornographic sites and news sites, shopping, stock trading, vacation planning, gaming, chatting, in other words, engaging in general non-business Internet activities on company time and using company resources.

3. Infantilization involves treating people as if they were still young children or condescension towards them.

4. Addiction implies psychological dependence on something (perhaps involving compulsive behavior) despite its (potentially) harmful effects.

5. Satisficing is choosing an option that is suboptimal, which seems justified because of the cost of finding or acting on the absolute maximal option.

6. Rationalization. This is the act of proposing reasons to justify one's behavior to satisfy oneself or an audience, however incorrect the reasons may be.

## The Issues

### Extent of the Problem

Cyberslacking in general would be adequate cause for concern on the part of employers, but a particular form of it is especially distressing to employers, namely, when employees use company time and bandwidth to seek other jobs. However, there might be value to top management in screening for this job seeking, e.g., to see if this activity is rife in a particular department; if so, that might call for special remediation in that department, which would ultimately benefit the company. (Drinkwater, 2000).

Two recent surveys (surfCONTROL website 2, 2000) give these results: "56% openly admitted to using the Internet for personal reasons while at work" (JSB's surfCONTROL and QuickTake.Com(SM)), and "Americans spent on the average 21 hours last month [Feb., 2000] (more than one hour per day) conducting personal Web surfing at work" (Nielsen-NetRatings). 32% acknowledged their job hunting activities on the web.

Additionally, the level of abuse is growing in severity: "Employees spent about one-third of their online time in recreation, a 1999 report from JSB's surfCONTROL shows. That was double the amount of online goofing off in 1998" (Griggs, 2000).

Still one might think that surfing the Internet is no different from gazing out the window while on the job. Caplan (2000) writes: "It [slacking] was going on before there ever was a computer on anyone's desk." However, the very power and cost of providing Internet service, as well as the quantity and cost of the risks involved put web surfing into a much different category. Slacking is not the only concern.

### Economic Effects

There are indirect costs as well: increased Internet use, beyond what is necessary for the business, requires purchase of additional bandwidth and consumption of unneeded resources. Increased Internet usage brings security problems as well. The more web sites visited unnecessarily (or even legitimately, of course), the greater

the exposure to viruses in the form of a malicious JavaScript and the like. Corporate intelligence is also at risk from unnoticed applets transmitting proprietary information and being more susceptible to being hacked. This exposure can rapidly escalate as employees exchange suspect URLs with one another causing additional logons.

A natural estimate of the cost of cyberslacking (based on research conducted by the Saratoga Institute of Human Resources) for just one hour per day of web surfing by 1000 internet users in a company is \$35 million each year. For the Fortune 1000 companies as a group, this cumulative 'one hour' could sum to \$35 billion (surfCONTROL website 1, 2000).

Finally the additional burden of dealing with downloaded images and movies can crash a company's network: In the case of Xerox, so many employees downloaded porn videos that it choked Xerox's vast computer network, to the extent of preventing other workers from opening or sending e-mail. "There were people spending all solid day doing nothing but clicking the mouse and downloading pictures," reported Xerox cybercop Mike Gerdes, who runs the company's eight member SWAT team on computer abuse (Naughton,1999).

Software downloaded from suspect Web sites could contain viruses or might represent copyright violations, the possibility that company secrets had been sent out over the Internet, and some unexpected company information, say employee files, being made available over the company's own Web site (Casser, 1996).

Ironically, cyberslacking creates yet an additional expense by causing the employer to purchase software to deal with the problem.

### **Moral Issues**

A fair extension of the notion of stealing to embrace more than property, but in fact anything whatsoever that is of value to an individual or organization, is in order. The time employees misuse, but for which they are compensated, as well as the monetary value of Internet access privileges via company equipment are properly considered objects of theft. Something of economic value is obviously being stolen.

Ralph Waldo Emerson discussed the type of theft relevant to cyberslacking in his essay, Compensation:

"In labor as in life there can be no cheating. The thief steals from himself. The swindler swindles himself" (Emerson, 1947). Clearly, the cyberslackers are depriving their company of the value of their services, and as the company's revenues decline, so do the chances of a decent bonus for the cyberslackers. Moreover, they might have to be laid off. Even worse, however—since Emerson tells only part of the story in order to appeal to the would

be thief's self-interest—the cyberslacker's actions also affect other workers and, of course, any shareholders negatively. Emerson's statement needs to be expanded: The thief swindles himself and innocent others.

If, however, the apparent Internet addict somehow still renders value to the company, perhaps even as a result of the cyberactivity, which might foster subconscious problem solving or provide a necessary break from drudgery or intense creative endeavor; there is obviously then no swindle. Naturally this somewhat exceptional case would have to be demonstrated to the employer. The employer ought then to make it known that this is an exceptional case and not necessarily the norm, so as not to create a precedent for all other workers not in this category. Here the employer would have to be both deft and fair in extending such privileges to all employees on a merit basis. Certain jobs, like producing a routine report on time, simply call for straightforward, consistent work, and not necessarily creative work. Hence there is an important distinction to be made about how time is spent in an environment of routine tasks or where the employee is constantly occupied versus an environment where work can be made up, say, in an end spurt. Time diverted to web surfing would be much harder to justify morally and practically, where routine tasks are the norm and lost time can not be made up. As a caution, one should note that nothing in this paragraph ought to be considered as reason to disregard the other problems engendered by cyberslacking.

### **Psychological Issues**

Rationalization. A worker once said: "I'm not cheating anyone. I'm a multitasker." "After all," she continued, "everyone shirks at work sometimes. Besides, what's more beneficial? Talking on the phone to a friend or maybe becoming more computer literate because you're using the computer?" (Naughton,1999). Her points may be substantially correct, but the behavior is nevertheless unjustified. What would she say if no one shirked at work? Another worker contends that " 'cyberslacking' can also be called catching up on personal business [which] a long workday denies." One must simply try to schedule the affairs of personal life on personal time, as a general rule. In the hierarchy of obligations, such employees claim (conveniently for themselves) that their lower level duties can reasonably supersede those at an obviously higher level. At a different time or place when other obligations did not trump their convenience, their explanations would be credible.

Infantilizing: Employee monitoring systems are fraught with difficulties for both those doing the monitoring and those being monitored. Here is the reaction of a person, who was "chastised" by a monitoring system about shopping on the Internet. She complained that the 'strongly worded' company e-mail warned ... she could be fired from work for cruising the Internet. "I felt

like I was back in first grade and the teacher thought I was cheating" (Naughton,1999). It has to be conceded that warning or punishing adults may be like dealing with young children, and a danger is that cyberslackers may regard themselves as still in the child mode of trying to get away with something until caught. Some solutions below deal with these problems.

**Guilt:** Cyberslacking can no doubt be the cause of guilt feelings. It may be symptomatic of an addiction, social incompetence away from the computer, and the like.

While everyone is free to seek alternate employment, most people would concede that it is particularly disloyal to use the resources of one's present employer to do so. Both the disloyalty and the surreptitious nature of the activity lead to guilt. Furtive activity breeds further guilt and often leads to a feeling of "I can get away with things (e.g., other misappropriations)."

**Stress:** Internet activities may be a welcome relief from stress, and for that reason, companies may wish to foster such activity, perhaps in the manner described above and also below in the remedies. On the other hand, excessive cyberslacking could in and of itself be the cause of stress, for instance, as one gets further and further behind in one's work. Then again, the ensuing guilt could bring on yet more stress.

**Addiction:** An ever-present danger to the employee who spends an inordinate amount of time web surfing is that he/she may become too habituated and dependent. In that case, the possibility of recovering and making up for lost time vanishes almost totally. If the Internet addiction also feeds on say an addiction to gambling on the web or pornography, there is a serious personnel issue, one that is costly to both the company and the employee.

## Legal Implications

Employees are often under the impression that they have privacy rights protected by the law when they engage in Internet activity. However, the courts have consistently decided that companies may be held liable for the e-mail messages and Internet activities of their employees (Rosenberg, 1999). Examples causing liability are misuse of copyrighted materials, leaking company or private information, and the like. Also, if an internal passerby sees objectionable material on a co-worker's screen, that too could lead to lawsuits, perhaps based on charges of creating a hostile environment.

The actions of employers to detect cyberslacking appear to be fully within the law and even legally protected. No corresponding safeguard exists for the employee. "With no general legal protection of workers' privacy, no actual protection exists. The courts have found little reason to challenge the determination, and

actual activities, of management to employ every means at its disposal to monitor the work, stationary and otherwise, of its workforce" (Rosenberg, 1999).

Recently, federal officials have initiated an investigation of some of the major players in e-commerce, such as, Amazon.com, eBay, and eToys. Internet advertising network because of their collecting consumer information (Wolverton and Sandoval, 2000). Conceivably they could share this information with employers, if they could be sure the employee/customer would always be in the dark. DoubleClick has also acknowledged a probe by the Federal Trade Commission into its practice of collecting customer information (Rosenberg, 1999).

## Proposed Solutions

An approach that appeals to the employee's sense of responsibility such as the one used by Texas Instruments (McManus, 1999) would go a long way to preventing feelings of being infantilized, while still exerting some moral influence. Their policy asks the employees to consider the legality of their computer activity, how it conforms to the company's values, if it seems wrong to the employee himself or herself, and how it would feel if the act were widely publicized. The strategy here is not only to have the employees police themselves, but to enlist their prior moral training and natural moral sensibilities. As a further back up, the employee is asked to imagine what the consequences of inappropriate behavior would probably be to themselves.

A correlative adjunct to showing faith and trust in the employees would be to have them form committees to formulate policies pertaining to internet usage. McManus (1999, p. 646) suggests forming committees to balance privacy concerns and company security. However, other committees might be concerned with balancing respect for employee freedom to work as seems most natural to the employee and the economic interests of the employer in light of the widespread tendency to use the web for healthy relaxation or occasional personal business, yes, even for moderate cyberslacking. Productivity might actually increase with such a corporate culture.

If the situation in a given organization seems to warrant it, the employer could choose to treat the problem as a moral or legal issue. First the employer would provide workshops involving an explanation of the moral issues of cyberslacking. The end result would then be to establish clear-cut company policies designed to avoid legal liability.

Another option open to the employer is to treat the problem of cyberslacking as a psychological disorder. Naturally, this would make sense only if there were excesses or evidence of compulsive behavior. Should the problem be compounded by feelings of self-reproach,

remorse, and stress caused by either running short of time or fear of being caught there are various treatment protocols for addiction, guilt, and tension. The employee could be referred or refer oneself to an appropriate counselor.

If there is no pressing psychological problem, the best approach might be some form of social redirection. A remedy for cyberslacking as an employee's substitute social activity might be to organize social functions where the cyberslacker is made to feel especially comfortable. This may even take the form of arranging social activities around the internet itself. An innovative human resources department could attempt to co-opt the tendency of the employees to surf while on the job by redirecting this propensity to "worthwhile" or edifying sites (areas that might inform or train the employees). Employees seem to agree that this would be a good thing, as one has said: "To be business savvy means understanding the Internet and you can't really do that unless you're online" (Fletcher, 2000).

This philosophy can be further encouraged by providing special equipment at the job site and even lend such equipment to the employees so they can surf the web at home. In this manner surfing can become a type of fringe benefit that both enhances the employee's knowledge or skill while simultaneously increasing morale as well as engendering loyalty to the organization—not to mention avoiding many of the ill effects of cyberslacking.

#### **Implementation of the Philosophy of Co-option**

- Announce that this activity, as long as it does not create problems for the company, will be continued if productivity does not decline.
- Confine surfing to lunch hours or personal time
- Award bonuses for bringing ideas to the organization from the web and learning new skills.
- Provide specific or random time slots (recesses) between 9 and 5 for personal surfing to relieve the dissonance and guilt, thereby removing the felt need to surf on designated company time.
- Create an "Acceptable Use Policy." For instance, an employee should agree to make up lost time due to surfing. If so, surfing would be permitted, provided individual performance is not lessened. The freedom to take such breaks might even lift both morale and productivity. A special contract would be drawn up specifying both the employee's rights and responsibilities with regard to computer usage.

The policy would contain understandable rules governing Internet access along with definite criteria to

determine whether a requested connection would be allowed or not. For example, the policy might provide that:

- (1) only designated persons, groups, workstations, or specific areas would be allowed non-business access,
- (2) time of access could be regulated
- (3) duration of access could be limited,
- (4) types of sites, both encouraged and prohibited, would be described, and
- (5) a statement of how much simultaneous access would be permitted in accordance with available bandwidth resources.

As a contributor to Newsweek [Messick, 1999] wrote, "Progressive companies that allow employees the occasional Web-surfing opportunity will be rewarded with lower absenteeism, higher morale and greater productivity." Here the operative word is "occasional"; perhaps one should add or even substitute the word, "reasonable."

#### **Control and Punishment**

A restrictive, theory X type of management might be deemed necessary in certain circumstances, say, if the lenient policies suggested failed. In such cases there would have to be increased supervision by managers or, better, by employees governing themselves.

- Co-worker or group reinforcement of company policy would be instituted to prevent cyberslacking, i.e., peer policing.
- Designate one employee to monitor the web usage of several others. This involves certain controlling behaviors, which are usually distasteful to managers and their designated subordinates, such as disciplining employees, encouraging snitching, and spying on employees.
- Making an example of those who are caught e.g., negative raises, firing. Companies expend a great deal "of money to train workers, and it's more efficient to keep an experienced employee than having to find and train a replacement" (Griggs, 2000). Thus the success of such tactics should be carefully examined. There are also economic drawbacks to be considered: "if the value of ... Web access control isn't significantly greater than the cost of the control mechanism, control doesn't make sense" (Gibbs, 1999).
- Remove the ability of employees to access the web either altogether or only in tightly controlled situations.

## Filtering

Ashley J. Phillips noted that filtering could offer businesses certain advantages over monitoring. For one thing, less labor is involved. Filtering prevents a person from logging onto objectionable sites, Phillips adds. No supervision is required when a company installs site-blocking software for corporate networks in particular if it uses artificial intelligence to identify and control which web addresses can be accessed. Such software utilizes "virtual control lists," employing "pattern matching to dynamically determine the context of a Web site and restrict access to it." There are also programs that not only allow employers to find out what sites their employees access but the amount of time involved (Griggs, 2000). This can help shape future policy on Internet access.

"Expert Filtering is a unique technology that combines three distinct filtering techniques: (Positive Filtering, General Filtering and Negative Filtering)" (SurfCONTROL web site 3, 1999). These will be discussed forthwith.

### Positive Filtering

There is a program, namely, SuperScout 2.5, that sorts "over 500,000 business URLs by their Standard Industrial Classification (SIC) code and then rate [s] their business relevance. Access is permitted or denied based on individual organizational policy and the Web site's relevance to the company's business" (SurfCONTROL web site 3, 1999). A company might even reward employees who bring ideas to the company from accessing relevant sites.

### General Filtering

This type of filtering takes into account those companies that might allow some recreational surfing at work, so such usage is permitted to URLs listed on a database of acceptable sites, such as those offering news, financial services, shopping, sports, and entertainment. A company can turn this type of access on and off during certain periods of the workday. "What's needed is a system that creates an acceptable Internet universe, letting employees know what Web sites they CAN go to, rather than where they CANNOT go," according to Steve Purdham (SurfCONTROL web site 3, 1999).

### Negative Filtering

There are Web sites that organizations should definitely prohibit their employees from visiting while on the job, and one would hope, even while off the job. Such offensive sites are those that are sexually graphic, prejudiced and otherwise demoralizing, which if visited on company equipment and during company hours – can detrimentally impact corporate morale and reputation. Moreover, it would not be a stretch to say that other employees might complain to various governmental

agencies that might subsequently levy fines, institute lawsuits, or impose unwelcome restrictions on the company.

## Philosophical Options.

It may very well be that even some "moral" battles are not worth fighting, in particular those involving the policing of employees. Here "worth fighting" does not pertain to economics or even management practices, but to the question of whether the principle involved is important enough to justify the effort. Whether such a choice is morally justified or not is still a matter of philosophical debate. Swanton (1993), for one, defends the thesis that "It is sometimes rationally preferable, perhaps even required to satisfy." Acting according to the virtue of providing a friendly environment for workers can be more rational than the absolute, act-oriented maximizing of profits.

One could argue that emphasis on a relatively minor peccadillo might come at the expense of preventing greater moral abuses, such as harassment or speculation. However, it should be recalled that embezzlement, revelation of company secrets, harassment, and neglect of security are also issues connected with cyberslacking. Still there is reason to believe that if an organization is careful about even minor moral issues, the employee would soon understand that breaches of higher obligations are going to be taken particularly seriously.

## Extension Of The Research

Some research topics related to organizational internet use and abuse, that could be treated in this same vein would be

- Dealing with hacking from the employers computer
- Establishing an organizational email policy with respect to privacy use for personal matters, harassment, etc.
- Being lax on security with regard to exposing the company to penetration or viruses
- The issues surrounding employees operating a private business on the employer's computer
- Video surveillance of work and restroom areas
- The non-business matter of the control of children's internet activities.
- The role of government (if any) in privacy issues within an organization, much like OSHA
- Proposals for protecting privacy in computer matters
- Collecting consumer information, with or without the knowledge and consent of the consumer

## References

American Heritage Electronic Dictionary, Houghton-Mifflin, version 3.0A 1992

Caplan, S. "Why Blame the Internet for Slacking?" *Letters*, Newsweek, New York, Dec 20, 1999.

Drinkwater, Dawn. Personal communication in my class on Mar.15, 2000.

Emerson, R. E. "Compensation" in The World's Great Thinkers, Man and Man: The social Philosophers, ed. Cummins, S. and Linscott, R. N., Random House, NYC, 1947, p. 439.

Fletcher, L. "PC benefit enhances skills, communication," Business Insurance; Chicago; Feb 28, 2000, Volume: 34, Issue: 9

Gibbs, M. "Counter points" Network World, Framingham; Dec 27, 1999-Jan 3, 2000; Vol. 17, Issue. 1, p. 99.

Griggs, T. "Web monitoring: Companies watching what workers watch," The Baton Rouge Advocate, 01/30/2000, p. 8-I

McManus, Y. "Ethics and Technology in the Workplace," *AMCIS 1999: Proceedings of the Fifth Americas Conference on Information Systems*, 1999, pp. 644-646.

Messick, T. "Clicking at work," *Letters*, Newsweek, New York, Dec 20, 1999.

Naughton, K. "Cyberslacking," Newsweek; New York; Nov 29, 1999, pp. 62-65.

Rosenberg, R. S. "The workplace on the verge of the 21st century," Journal of Business Ethics; Dordrecht; Oct 1999, pp. 3-14.

<http://news.excite.com/news/bw/000306/ca-jsb-surfcontrol?printstory=1>, 2000, (Current Mar. 15, 2000).

"Cyberslacking at Work Continues to Threaten Productivity Survey Zeroes in on Newest 'Internet Distractions'," [http://www.surfcontrol.com/news/in\\_the\\_press/pressreports/introweek021700.html](http://www.surfcontrol.com/news/in_the_press/pressreports/introweek021700.html), (Current Mar. 15, 2000).

Internet Market Press Release: "JSB's "Raises The Stakes" In Corporate Internet Filtering Marketplace" [http://www.surfcontrol.com/news/press\\_releases/15-03-1999\\_2.html](http://www.surfcontrol.com/news/press_releases/15-03-1999_2.html), 1999, (Current Mar. 15, 2000).  
Wolverton, T. and Sandoval, G. "Probes are latest headache in e-commerce," CNET News.com, February 16, 2000, 1:00 p.m. PT <http://news.cnet.com/news/0-1007-200-1551662.html>, (Current Mar. 15, 2000)

Swanton, C. "Satisficing and Virtue," The Journal of Philosophy, Vol. XC, #1, Jan. 1993, p. 35.